AFFIDAVIT OF SPECIAL AGENT CASEY ANDERSON IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Casey Anderson having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since September of 2019. I am assigned to the Springfield, Massachusetts (MA) Resident Agency of the FBI, Boston Division, where I am responsible for conducting federal fraud investigations, including wire fraud, and conducting other investigations related to white collar crime. My participation in these investigations has included utilizing confidential informants and cooperating witnesses; coordinating and conducting the execution of search and arrest warrants; performing victim and witness interviews, reviewing financial records and documents, and conducting electronic and physical surveillance.

2. The FBI is currently investigating Richard Duncan ("Duncan") for violations of 18 U.S.C § 1343 fraud by wire radio or television.

3. I submit this affidavit in support of an application for a warrant under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure to search and seize records and data from the e-mail accounts identified as **RD01106@gmail.com** ("the target account") described in attachment A.

4. I have probable cause to believe that these accounts contain evidence, fruits, and instrumentalities of the crimes identified above, as described in Attachment B.

5. Based on the e-mail address's domain name, I have probable cause to believe that the accounts and relevant data are maintained by Google Inc. ("Google"), which, government databases indicate, accepts service of process at:

Lers.google.com

as described in Attachment A.

6. The statements contained in this affidavit are based upon my investigation, statements made in interviews, photographic evidence, and on my own experience as a Special Agent of the FBI. Because this affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C § 1343 fraud by wire radio or television, identities of victims, and/or information related to identities of conspirators not yet identified will be obtained through the collection of the content of electronic communication for the Gmail account **RD01106@gmail.com.**

LEGAL AUTHORITY

7. The government may obtain both electronic communications and subscriber information from an e-mail provider by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A). Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the website hosting company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g). If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3). This application seeks a warrant to search all responsive records and information under the control Google subject to the jurisdiction of this court, regardless of where Google has chosen to store such information.

Pursuant to 18 U.S.C. § 2713, the government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

INTRODUCTION TO THE FRAUDULENT SCHEME

8. This affidavit describes some of the facts gathered through an ongoing investigation that has revealed an advance fee fraud scheme perpetrated by an individual believed to be Richard Duncan (Duncan), and others not yet identified, in which individuals were recruited into an investment venture, promised high rates of returns on their investments, and instructed to send money to individuals in the United States and overseas. This pattern was repeated and additional requests for more money were provided to Duncan. Duncan then recruited victims, who provided money to Duncan to fund the fraudulent investments or sent payments directly to coconspirators as yet unknown. Duncan, who was a licensed investment advisor, actively recruited investors from a series of former clients and close friends. According to statements from victims, Duncan was successful in collecting investments due to the trust these individuals placed in him, resulting from their long associations with Duncan and Duncan's perceived professional expertise. Due to his fraudulent investments, Duncan was fired from investment firms; had his access to a trading platform rescinded; and was subject to enforcement action from the United States Securities and Exchange Commission (SEC). Duncan was notified of the fraudulent nature of his investment activities overseas by the SEC, by financial institutions, and by currency remittance companies. Despite these warnings and consequences,

Duncan continued to attempt to recruit investors and send funds overseas. Most recently, Duncan has sent $247,600.00 that originated from a Payment Protection Plan (PPP) Loan from the Small Business Administration (SBA), from his bank account to others at the direction of coconspirators. Duncan is a resident of Springfield, Massachusetts. Duncan's victims are residents of Massachusetts and Connecticut.

9. From August of 2016, until this date more than 40 transfers of currency have been completed between Duncan, or victims acting on Duncan's behalf, to coconspirators connected with the fraud scheme located in Istanbul, Turkey and other locations located in and outside the United States. These transactions were often structured to avoid mandatory reporting requirements or daily transfer limits of financial institutions. Transactions have been completed using multiple means including wire transfer from financial institutions, remittance services like MoneyGram, the purchase and mailing of cashier's checks, and the sending of cash through the United Parcel Service (UPS) or Fedex.

PROBABLE CAUSE TO BELIEVE A FEDERAL CRIME WAS COMMITTED

Recruitment of Duncan and Victims into the fraudulent investment scheme

10. The FBI began an investigation into Duncan's participation in an advance fee scheme in January of 2019. Interviews with victims and associates of Duncan and documents obtained from the US Securities and Exchange Commission (SEC) during their initial investigation indicated that during or around August of 2016, Duncan was contacted by individuals yet unknown, who facilitated an introduction with other individuals as yet unknown, who claimed to be a woman who lived in Turkey named Janet Marck (Marck) and her lawyer Richard Morgan (Morgan). According to interviews with victims, interviews with Duncan conducted by the SEC, and messages collected between Duncan and Victim 3, the individual

claiming to be Marck solicited Duncan with the opportunity to manage financial assets of nearly 6 million US Dollars (USD) if Duncan could assist Marck in bringing her money to the United States. Marck asked Duncan to provide money for a series of fees and personal financial setbacks that were preventing Marck from making progress in moving money. Marck asked Duncan to provide money to book a cargo ship to transport trunks full of money from Turkey to Boston, Massachusetts (Herein known as "the Turkish Investment"). At some point, Duncan exhausted his own resources, and solicited clients from his financial advising business to provide money to be sent to Marck, with the promise of between 20% to 100% returns on their investments. In interviews with the SEC, Duncan has failed to demonstrate compliance with any due diligence and disclosure requirements required by his position as a financial advisor. Duncan admitted to the SEC that he did not provide documentation for investments. Duncan's participation in the Turkish investment broke rules established by his employing institutions that led to his termination. Additionally, two of the investors Duncan selected were suffering from diminished mental capacity. According to Duncan, Duncan has Power of Attorney for Victim 2, who has addiction and alcoholism issues. Victim 1, suffers from a form of dementia, and Duncan failed to consult the individual with Enduring Power of Attorney for Victim 1 on several occasions when seeking money from Victim 1. Additionally, Duncan and Victim 1 circumvented the authority of the individual with Enduring Power or Attorney over Victim 1 on at least one occasion after the individual restricted Victim 1's access to funds. Duncan and Victim 1 were able to withdraw additional funds from multiple accounts and send additional money overseas as part of the fraudulent investment. Duncan used email, text messaging, and other methods to communicate instructions to his victims; to coordinate the movement of money; and to communicate with individuals as yet unknown who provided instructions on where to transfer money,

communicated pertinent points of the narrative shared with victims, and articulated needs for additional money. To date, neither Duncan nor any of Duncan's victims have seen the return of any funds.

11. Since Duncan was notified that his investments in the Turkish investment were fraudulent, Duncan has continued to solicit money from his victims and make additional promises of financial return, circumvent financial institutions safeguards against fraud, and used email as a primary means of communicating with victims and coconspirators. Additionally, as victims have been identified and notified about the fraudulent nature of the Turkish investment, Duncan has sought new ways to fund transfers of money to his coconspirators in Turkey.

Transfers of Currency to Turkey

12. On September 21, 2020 the SEC conducted an interview with DUNCAN ("the SEC interview") DUNCAN provided a more complete description of transactions related to the Turkish Investment. During the SEC interview DUNCAN explained that prior to August of 2016, Marck had requested DUNCAN's assistance with managing an inheritance, however, in August, Marck began requesting money for other reasons. Duncan explained, "so at this point in time, I'm getting back to Janet, she said well, we're going to need some money. I can't get my hands on it. I don't know what I'm going to do. My son is not doing well. There's a chance he's going to need some surgery." As a result, DUNCAN provided funds to other individuals on behalf of Marck.

13. Between August 15, 2016 and September 27, 2016 Duncan transferred approximately $20,970.00 USD to Moneygram accounts for Ballard Zimba (Zimba), Andrew Evans (EVANS), or Allen Andy (Andy) located in Istanbul, Turkey through multiple transactions. Transaction information is as follows:

a. On August 15, 2016 at approximately 10:40 AM[1] Duncan transferred $2000.00 USD to ZIMBA via MoneyGram from CVS #517 in Longmeadow, MA.

b. On August 15, 2016 at approximately 11:22 AM DUNCAN transferred $400.00 USD to ZIMBA via MoneyGram from CVS #1130 in Springfield, MA.

c. On August 21, 2016 at approximately 8:02 AM DUNCAN transferred $250.00 to ZIMBA via MoneyGram from CVS #355 in Newport, RI.

d. On August 22, 2016 at approximately 1:44 PM DUNCAN transferred $2000.00 to ZIMBA via MoneyGram from CVS #517 in Longmeadow, MA.

e. On August 22, 2016 at approximately 2:27 PM DUNCAN transferred $2000.00 to ZIMBA via MoneyGram from C-Mart in East Longmeadow, MA.

f. On August 22, 2016 at approximately 2:39 PM DUNCAN transferred $520.00 to ZIMBA via MoneyGram from CVS #1130 in Springfield, MA.

g. On September 2, 2016 at approximately 1:11 PM DUNCAN transferred $2000.00 to EVANS via MoneyGram from CVS #517 in Longmeadow, MA.

h. On September 2, 2016 at approximately 1:42 PM DUNCAN transferred $2000.00 to EVANS via MoneyGram from CVS #1130 in Springfield, MA.

i. On September 2, 2016 at approximately 2:01 PM DUNCAN transferred $2000.00 to EVANS via MoneyGram from C-Mart in East Longmeadow, MA.

j. On September 2, 2016 at approximately 2:31 PM DUNCAN transferred $2000.00 to EVANS via MoneyGram from CVS #1157 in Springfield, MA.

k. On September 2, 2016 at approximately 3:02 PM DUNCAN transferred $2000.00 to EVANS via MoneyGram from CVS #2566 in Wilbraham, MA.

---

[1] All times for MoneyGram transfers in Eastern Standard Time.

l. On September 24, 2016 at approximately 9:01 AM DUNCAN transferred $2000.00 to Andy via MoneyGram from CVS #1157 in Springfield, MA.

m. On September 24, 2016 at approximately 9:23 AM DUNCAN transferred $1800.00 to Andy via MoneyGram from CVS #2566 in Wilbraham, MA.

14. Based on my training and experience, I know that criminals often structure money financial transfers in a way that allows them to avoid reporting requirements for financial institutions and daily or monthly caps placed on customers transfer amounts of frequency. Some structuring strategies included making currency transfers from multiple locations same day, transferring money to multiple recipients, and breaking up larger currency transfers into smaller individual transfer amounts. Duncan exhibited typical structuring patters while using MoneyGram in August and September of 2016. Despite the attempt to structure currency transfers to avoid fraud detection, Duncan admitted during the SEC interview that MoneyGram created problems for the Turkish Investment because MoneyGram identified the transactions as "a scam."

15. During the SEC Interview Duncan claimed that he transferred approximately $100,000.00 USD to the Turkish Investment prior to recruiting any additional investors. Duncan described his participation in the Turkish Investment during the end of 2016 saying, "We get through September. We're now in October. I'm now fully committed to trying to help this woman in a serious kind of way, and between September and the end of the year, if my memory is -- correct me, I could be wrong about this, if you get me in court and it's treated differently -- maybe I should just through a little caveat on this particular thing, but I'm pretty sure that by the end of the year, I had provided well over $100,000. And over the next several months, that became $200,000 that I had in savings, in cash, in a safe. And the -- and as we stand right now, a

few years later, I have about $300,000 invested, but $200,000 were invested before [Victim 1] even – [Victim 1] even got involved with this or was part of a conversation because I didn't really think any of that was going to be necessary." Duncan continued by explaining that he warned Victim 1 that the Turkish Investment may have been a scam, but that it also could lead to a 100% return on investment. Duncan described Victim 1's initial investment saying, "So he started off with, I think, $17,000 or $19,000, the heavy money didn't come until later."

Victim 1

16. As set forth below in more detail, my interview with Victim 1, Witness 1, bank records, and other information all show that Duncan caused Victim 1 to provide approximately $300,000 to the Turkish Investment. This was done typically through a series of circuitous financial transactions that seem to have been designed to obfuscate the money trail.

17. On September 22, 2020, I interviewed Victim 1. During the interview, Victim 1 confirmed that Victim 1 had provided approximately $300,000.00 USD to the Turkish Investment. Victim 1 explained that Victim 1 had expected a 100% return on investment. Victim 1 also explained that the decision to fund the Turkish Investment was based on Victim 1's trust in Duncan and Duncan's good business sense.

Victim 1 Financial Transactions with Turkish Investment

18. On January 11, 2017, Victim 1 withdrew $16,000.00 USD from a United Bank account ending in 1511. On the same date, Duncan deposited $15,800.00 USD into a Bank of America (BOA) account ending in 2012. Later that same day (January 11, 2017), Duncan transferred $15,800.00 USD to Andy's AKBANK account ending in 6349. AKBANK is a Turkish Bank that Duncan describes as a recipient bank in the Turkish Investment currency transfers. Based on the interview with Victim 1 and the bank records, it appears that $15,800 of

Victim 1's $16,000 was given to the Turkish Investment and Duncan kept $200.

19. On January 25, 2017, Victim 1 withdrew $21,000.00 USD from a United Bank account ending in 1511. On the same date, Duncan deposited $21,000.00 USD into a BOA account ending in 2012. On January 25, 2017 Duncan transferred $21,000.00 USD to Andy's AKBANK account ending in 6349. Based on the interview with Victim 1 and the bank records, it appears that all of Victim 1's $21,000 was given to the Turkish Investment.

20. On March 1, 2017 Victim 1 cut two checks from a United Bank account ending in 5401, each made out to "Cash." Check number 2906 was for $6,500.00 USD. Check number 2907 was for $1,000.00 USD. Later on March 1, 2017, Duncan deposited $7,860.00 USD into a BOA account ending in 2012. On the same date Duncan transferred $7,800.00 USD to Andy's AKBANK account ending in 6349. Based on the interview with Victim 1 and the bank records, it appears that all of Victim 1's $7,500 was given to the Turkish Investment and $300 was provided to the Turkish Investment from another source.

21. On September 25, 2020, I Interviewed Witness 1, the wife of Victim 1. Witness 1 explained that Victim 1 initially provided $16,000.00 to DUNCAN for an expected 100% return on investment. Witness 1, approximated the date of the initial transaction to summer of 2016. Investigators have since used bank records to identify the correct date of the initial $16,000.00 transaction as January 11, 2017 as referenced in paragraph 17. Witness 1 told investigators that within months of being told about Victim 1's involvement in the Turkish Investment, Witness 1 identified a home equity line of credit and said that Victim 1 had withdrawn approximately $100,000.00 of that credit and provided the funds to Duncan for the Turkish Investment.

22. Witness 1 provided a transaction summary from the home equity line of credit from United Bank referenced in paragraph 20. The transaction report shows 10 withdrawals

totaling $133,989.00 USD occurring between March 10, 2019 and August 7, 2019. Several of these withdrawals correspond to transactions in the Turkish Investment that are known to investigators. Those transactions are described below.

23. On March 10, 2017, Victim 1 withdrew $15,000.00 USD from the United Bank line of home equity line of credit. On the same date, Duncan withdrew $350.00 USD from a Berkshire Bank account ending in 6440. Later that day, Duncan deposited $18,100.00 USD into a BOA account ending in 2012. Duncan transferred $18,000.00 USD to Andy's AKBANK account ending in 6349 from the BOA account ending in 2012. Based on the interview with Witness 1 and the bank records, it appears that Victim 1's $15,000 was given to the Turkish Investment and $3,000 was obtained from another source for the Turkish Investment.

24. On March 29, 2017, Victim 1 withdrew $9,000.00 and $6,000.00 USD from the United Bank line of home equity credit in two separate transaction. On the same date, Duncan deposited $15,000.00 USD into a Berkshire Bank account ending in 6440. Later on March 29, 2017 DUNCAN transferred $14,400.00 USD to a beneficiary name Mercy Stowe (Stowe). Account information for Stowe's bank account used in this transaction was not available, but numerous other transactions conducted through MoneyGram and related to the Turkish Investment showed the recipient location for Stowe was located in Istanbul, Turkey. Based on the interview with Witness 1 and the bank records, it appears that $14,400 of Victim 1's $15,000 was given to the Turkish Investment and Duncan kept $600.

Victim 2 and Victim 3

25. A review of financial records reveals that Victim 2 and Victim 3 became involved in the Turkish Investment in August or September of 2017. Victim 2 is the parent of Victim 3. Victim 2 has a history of alcoholism and was arrested on December 21, 2020 for a violent

altercation involving Victim 3 and another individual. Police reports from the incident that Victim 3 explained to officers that Victim 2 had recently been diagnosed with Alzheimer's.

26. In the SEC interview, Duncan described the involvement of Victim 2 in the Turkish Investment. Duncan explained that due to Victim 2's alcohol and drug addiction, Duncan had received power of attorney for Victim 2 and was acting as the trustee for Victim 2's investments. Duncan explained that Victim 2 would often provide Victim 3 with money that Victim 3 would use to purchase drugs. Duncan, therefore, approached Victim 2 with the Turkish Investment to limit Victim 3's ability to access Victim 2's money and as a lucrative investment option. Duncan attests that Victim 2 was in a state of sobriety and was, therefore, lucid enough to consent to providing funds to the Turkish Investment.

27. Duncan had control, acting as a trustee, of multiple TD Ameritrade accounts for Victim 2, including accounts number 925-317294, which was opened by Duncan on August 22, 2017. Numerous transactions related to the Turkish Investment have been conducted by Victim 2 or involving Victim 2's accounts. Selected transactions are described below, but the full loss amount for Victim 2 is not yet known.

28. The first transaction known to investigators involving funds from Victim 2 occurred on September 14, 2017. During this transaction Victim 2 used MoneyGram to transfer $2000.00 USD to Larry Kesher (Kesher) from C-Mart in East Longmeadow, MA. Kesher's receiving location was in Istanbul, Turkey.

29. On October 10, 2017, Victim 2 received $2000.00 USD in a BOA account ending in 9889 from TD Ameritrade account 925-317294. The transaction listed the receiving party as "DUNCAN RICHARD." The same day Victim 2 used MoneyGram to transfer $1850.00 USD to Stowe from CVS 1157 in Springfield, MA.

30. On October 20, 2017 Victim 2 used MoneyGram to transfer $1000.00 USD to Sheldon Weisberg from CVS 1157 in Springfield, MA. Weisberg's receiving location was located in Istanbul, Turkey. On the same day Duncan transferred $2000.00 USD to Weisberg from CVS 1130 in Springfield, MA.

31. On December 29, 2017, Victim 2 received $2500.00 USD in a BOA account ending in 9889 from TD Ameritrade account 925-317294. The transaction listed the receiving party as "DUNCAN RICHARD." On December 31, 2017 DUNCAN used MoneyGram to transfer $2000.00 USD to Gabriel Donald (Donald) from CVS 517 in Longmeadow, MA.

32. On January 21, 2018 Victim 2 wrote a check number 286 from the BOA account ending in 9889 for $19,000.00 USD made payable to Richard G. Duncan. On January 24, 2018 DUNCAN deposited check 286 into his Berkshire Bank account ending in 6440. On January 26, 2018 a deposit return for $19,000.00 USD occurred in DUNCAN's Berkshire bank account ending in 6440. The same account then had $19,000.00 USD removed from the account and received a retuned check fee of $7.23 USD. On January 25, 2018, following the failed attempt to deposit $19,000.00 USD into Duncan's account via check, a transfer of $19,500.00 USD from TD Ameritrade account 925-317294 to Victim 2's BOA account ending in 9889 occurred. On January 29, 2018, following receipt of the funds, Victim 2 withdrew $19,000.00 USD from the BOA account ending in 9889 and purchased a BOA cashier's check number 1461505928 for $19,000.00 USD made payable to "Richard C. Duncan". On January 29, 2018, BOA cashier's check number 1461505928 posted. On the same date, DUNCAN cashed BOA cashier's check number 1461505928 and received $3,000.00 USD in cash, and BOA cashier's check 1461505931 for $16,000.00 USD made out to "Richard G. Duncan". On January 30, Duncan deposited BOA cashier's check 1461505931 for $16,000.00 USD into his Berkshire Bank

Account ending in 6440. Duncan withdrew $18,200.00 USD from his Berkshire Bank Account ending in 6440 on February 16, 2018.

33. On February 3, 2018 Victim 2 and Victim 3 opened a BOA bank account ending in 3773. The BOA account ending in 3773 has received numerous deposits from a TD Ameritrade account with an as yet unknown account number and a receiving party listed as "DUNCAN RICHARD." Some of these transfers were followed by cash withdrawals or the purchase of cashier's checks that listed names of individuals known or believed to be connected to the Turkish Investment. Several of those transactions are described below.

34. On May 16, 2018, Victim 2 and Victim 3 received a transfer of $12,500.00 USD into the BOA account ending in 3773 from the unknown TD Ameritrade account. The transaction listed the receiving party as "DUNCAN RICHARD." Later that day Victim 2 and Victim 3 withdrew $10,000.00 USD from the BOA account ending in 3773. The withdrawal slip used during the transaction includes a note listing the name Olufemui Sadiq (Sadiq).

35. When asked about the identity of Sadiq in the SEC Interview, Duncan said that Sadiq was "a link in the chain," i.e., that Marck had told Duncan to send money to Sadiq. Duncan also explained that Sadiq was the CEO of a company called Date2Marry and that Sadiq was located in Texas.

36. On September 27, 2018, Victim 2 and Victim 3 received a transfer of $18,000.00 USD into the BOA account ending in 3773 from the unknown TD Ameritrade account. The transaction listed the receiving party as "Duncan Richard." On September 28, 2018, Victim 3 withdrew $4,100.00 USD and $12,010.00 USD in two transactions from the BOA account ending in 3773. The withdrawal slip used during the $12,010.00 USD transaction includes a note listing the name Ruth Burstein (Burstein).

37. On November 14, 2018, Victim 3 received $5,900.00 USD from a TD Ameritrade account into a United Bank Account ending in 4076. On the same date Victim 3 withdrew $4,150.00 USD from the United Bank Account ending in 4076. At approximately 1:41 P.M. on November 14, 2018, Victim 3 cashed a cashier's check for $1,720.00 USD at United Bank. Victim 3 was then charged a $10.00 USD fee for cashing a cashier's check. Following that transaction, Victim 3 purchased cashier's check 619820 for $5,850.00 USD and was charged a $10.00 USD cashier's check purchasing fee. The amount of the cashier's check 619820 ($5,850) was equal to the total of the amount withdrawn from the United Bank Account ending in 4076 ($4,150), plus the amount for the cashier's check cashed by Victim 3 ($1,720), minus the two $10.00 USD fees charged by United Bank. Cashier's check 619820 listed Victim 3 as the remitter and was made out to Sadiq. On December 13, 2018 Duncan cashed United Bank cashier's check 619820, made out to Sadiq.

38. On January 18, 2019, $46,000.00 USD was transferred from a TD Ameritrade account for Victim 2 and Victim 3 to Victim 3's United Bank account ending in 4076. On January 29, 2019, Victim 3 withdrew 45,000.00 USD from the United Bank account ending in 4076 after a previous failed attempt to withdrawal the funds. Investigators believe this withdrawal was also connected to the Turkish investment.

Victim 4

39. Investigators interviewed Victim 4 multiple times in 2020. During those interviews Victim 4 explained the following facts. Duncan recruited Victim 4 into the Turkish Investment in the summer or fall of 2019. Victim 4 only provided money directly to Duncan or sent money to an individual using the name Henry Franssen (Franssen) for the Turkish Investment. Victim 4 has lost approximately $140,00.00 USD to the Turkish Investment.

Victim 4 has given the majority of that money directly to Duncan. Victim 4 claimed that all money given to the Turkish Investment was transferred out of Victim 4's bank account at Franklin First Federal Credit Union (FFFCU), ending in 9104.

40. A review of financial documents has shown that Victim 4's participation in the Turkish Investment, knowingly or unknowingly, may have actually begun earlier in 2019. Several of the transfers or withdrawals Victim 4 made for Duncan or others in the Turkish investment are outlined below.

41. On March 20, 2019, Victim 4 withdrew $3,000.00 USD from the FFFCU account ending in 9104 and listed "R. Duncan" on the deposit slip. Victim 4 made numerous other withdrawals between March 20, 2019 and June 29, 2020 from the FFFCU account ending in 9104.

42. On October 30, 2019, Duncan deposited $2,000.00 USD into Duncan's TD Bank account ending in 3720. On November 1, 2019, Victim 4 transferred $1,200.00 USD Victim 4's FFFCU account ending in 9104 to Duncan's TD Bank account ending in 3720. On November 4, 2019 Duncan transferred $3,200.00 from Duncan's TD Bank account ending in 3720 to Franssen's Bank of Melbourne account ending in 4446.

43. On November 21, 2019, Victim 4 transferred $6,000.00 USD from the FFFCU account ending in 9104 to a TD Bank account ending in 3720 owned by Duncan. On November 22, 2019 DUNCAN transferred $6,000.00 USD from TD Bank account ending in 3720 to Franssen's Bank of Melbourne account ending in 4446.

44. On December 20, 2019, Victim 4 transferred $4,000.00 USD from the FFFCU account ending in 9104 to a TD Bank account ending in 3720 owned by Duncan. On December 23, 2019 Duncan transferred $4,000.00 USD from TD Bank account ending in 3720 to

Franssen's Bank of Melbourne account ending in 4446.

45. On January 13, 2020 and January 14, 2020 Victim 4 transferred $10,000.00 USD from the FFFCU account ending in 9104 directly to Franssen at an ANZ Bank account ending in 1011 using two requests.

46. On February 25, 2020, Victim 4 transferred $14,000.00 USD from the FFFCU account ending in 9104 directly to Franssen at an ANZ Bank account ending in 1011. Victim 4 listed "personal" as the reason for the transfer.

47. On February 28, 2020, Victim 4 transferred $7,000.00 USD from the FFFCU account ending in 9104 directly to Franssen at an ANZ Bank account ending in 1011. Victim 4 listed "personal" as the reason for the transfer.

48. On March 6, 2020, Victim 4 transferred $2,400.00 USD from the FFFCU account ending in 9104 directly to Franssen at an ANZ Bank account ending in 1011. Victim 4 listed "loan" as the reason for the transfer.

SBA Loan

49. The above noted transactions are not the only transaction related to the Turkish Investment known to investigators.

50. Duncan also used funds from a Small Business Administration (SBA), Paycheck Protection Plan (PPP) Loan to provide funds for the Turkish Investment. On July 7, 2020, the SBA deposited $113,800.00 USD into Duncan's TD Bank account ending in 3720. The bank statement for the account ending in 3720 clearly listed the source of the funds as "SBAD TRES 310." On the same, day Duncan withdrew $48,678.00 USD from the TD Bank account ending in 3720. Duncan then purchased cashier's check 31811074-7 for $48,678.00 USD made out to Steven R. Hull (Hull) with a Chase Bank account ending in 0395 and a routing number of

035000019. On July 8, 2020 Duncan made a withdrawal for $2,000.00 from the TD Bank account ending in 3720 and wrote a check for $8,000.00 USD to "Richard Duncan" listing a request on each stating "large bills please." Later on July 8, 2020, Duncan withdrew $53,592.00 USD from the TD Bank account ending in 3720 and purchased cashier's check 31811084-8 for $53,592.00 USD made out to Steven R. Hull with a Chase Bank account ending in 0395 and a routing number of 035000019.

51. Hull was interviewed by investigators in February of 2021. In the interview, Hull explained that he has met a person online that claimed to be Traci Bush (Bush). Hull had never met Bush in person, but explained that they communicated via messenger apps, and on the phone on one occasion. Hull then described a series of events that match the common pattern of a romance scam, including sending money to Bush, opening bank accounts at the request of Bush, and purchasing bitcoin for Bush.

52. Based on my training and experience, I know that individuals involved in financial fraud often use numerous individuals to transfer money through a complex network of people in order to make it difficult for investigators to identify the source and end recipients of fraudulently obtained funds. Individuals involved in these transactions are often referred to as "money mules." Money mules are often convinced to send money by using a number of different fraudulent schemes, like romance scams and work-from-home-scams. Hull's activities are consistent with an individual who has fallen victim to a romance scam and that has been recruited into a money mule network.

53. On July 14, 2020, the SBA deposited $149,900.00 USD into Duncan's TD Bank account ending in 3720. The bank statement for the TD Bank account ending in 3720 clearly listed the source of the funds as "SBAD TRES 310." On the same, day Duncan withdrew

$59,619.00 USD from the TD Bank account ending in 3720. Duncan then purchased cashier's check 31811115-3 for $59,619.00 USD made out to Denise Boyd Merchell. On July 15, 2020, Duncan withdrew $10,000.00 USD from the TD Bank account ending in 3720. On July 16, 2020, Duncan withdrew $63,323.00 USD from the TD Bank account ending in 3720. Duncan then purchased cashier's check 31811123-2 for $63,323.00 USD made out to Denise Boyd Merchell. That same day, Duncan also withdrew $10,000.00 USD from the TD Bank account ending in 3720.

54. Denise Boyd (Boyd), formerly Denise Boyd Merchell, was interviewed by investigators, Boyd was involved in a scam in which she provided money to an individual claiming to be Alice Herem (Herem). At some point Herem informed Boyd that Boyd worked for Duncan as part of the scam. Boyd refused to work for anyone because Boyd was on disability. Boyd spoke to Duncan on the telephone from phone number (413) 348-9896. Duncan told Boyd that she now worked from Duncan. Boyd provided a written account of her interactions with Duncan in which she explains that Duncan also called Citizens Bank and told the bank that Boyd was an employee of Duncan. Boyd received $59,619.00 USD into a Citizens Bank account ending in 0792 on July 30, 2020. Boyd believe the money was a government grant, but Duncan told her the money was not a grant.

The use of the Gmail Account

55. Information gained from interviews with multiple victims, interviews conducted by the SEC with Duncan, and text messages exchanged between Duncan and Victim 4 has confirmed that that email is the primary method of communication used by Duncan to communicate with coconspirators and is commonly used by Duncan to communicate with the victims on matters related to the fraud scheme. Specifically, interviews with Victim 1 and

Victim 4 have indicated that Duncan communicated instructions or updates related to the fraud scheme to them via email. Victim 4 also explained that Duncan forwarded documents to Victim 4 via email, that were purportedly sent to Duncan by Marck and the Chairman of Turkish Kargo (The Chairman).

56. Emails were sent directly to Victim 1 from the email address RD01106@gmail.com. Victim 1 allowed investigators to review and document the content of some of these email messages. The emails wiring instructions and email addresses for individuals instructing Duncan on where to transfer money including: Janet_marck@yahoo.com, turkishkargo1@gmail.com, richardmorganchambers@mail.com, janetmarck801@gmail.com, richardmorganchambers94@gmail.com, and marckjanet@gmail.com.

57. During the SEC Interview, Duncan provided statements that demonstrate the consistent use of email to communicate information directly related to the fraudulent investment with coconspirators and victims.

58. When asked about Duncan's relationship with Marck, Duncan outlined his first communication via email with Marck, in 2016.

> DUNCAN: …we're at the end of July, early part of August and if my memory serves me correctly, that's about the time I get my first email from Janet Marck. And she's introducing herself. She's acknowledging the fact that I've been talking to her attorney. And she wants to let me know that what he has told her is something that seems like a good thing to do and, you know, she'd be interested in, you know, talking to me…

59. When SEC investigators asked Duncan how many calls Duncan had with the individual claiming to be Morgan, the attorney representing Marck in the Turkish investment scheme, the following exchange occurred.

SEC: So, how many calls did you have with this attorney from Turkey?

DUNCAN: How many emails would I have received? Because that's how we communicated.

SEC: I guess -- okay, it was all by email. Did you ever speak to him on the phone?

DUNCAN: Yes, but it would always be that he would call me, but I -- but I did speak with him, you know, actually fairly frequently.

60. For clarification, the SEC asked Duncan if he had retained communications between Duncan and Morgan. Duncan responded as follows.

DUNCAN: Do I still have the emails? Is that what you just said?

SEC: Yes.

DUNCAN: Yes, I do. I just got to -- I just -- you know, they're not easy to find, but I know I have them.

61. When asked about the logistics of moving money Duncan discussed his conversations with an individual claiming to be Robert Longman, a representative of the Turkish Akbank. Duncan reported that this individual represented the bank and was the head of its wire transfer department. The following exchange occurred during the SEC interview:

SEC: And when you would talk to Mr. -- was it Longman -- Longman -- Langman?

DUNCAN: I did everything with email through him, too. Okay, but that was my --

SEC: "Did you ever speak to Mr. Langman on the phone?"

DUNCAN: "No I didn't get him on the phone but I have letters."…

62. The following statement occurred when Duncan clarified the contents of those letters.

DUNCAN: And some of them are emails to the attorney, which are -- you know, I could

get to you. And some of them are emails with Phillip Longman that I thought were important enough to keep, and I'm pretty sure I kept them.

63. When asked about due diligence requirements related to Duncan's position as an investment advisor and the steps Duncan took when verifying the identity of Marck, Duncan and the SEC had the following exchange:

SEC: … You never met her is that right?

DUNCAN: No, I've never met her. Okay. I have her email as well, yeah. have her email -- well, yeah, I mean we must've had at least 200 hours of email conversations with each other. And initially, we used Facebook; then we changed to something else and so forth… But I had -- I had hours upon hours upon hours upon hours of discussions with her. She's also got an email address, which I can give you to you.

64. In the interview with the SEC, DUNAN also referenced likely using email to obtain copies of Marck's bank statements from either Marck or Morgan; receiving copies of Marck's father's will from Morgan via email; and receiving invoices and other documentation from other coconspirators via email.

65. Text messages between Duncan and Victim 4 demonstrate that email is a consistent form of communication between Duncan and those he has convinced to participate in the fraudulent investment scheme. Numerous text messages reference exchange of information related to the fraudulent investment scheme being conducted over email. A selection of those text messages reads as follows:

66. Text message exchange between Duncan and Victim 4 on November 23, 2018:

Duncan: … can you call me when you get in tomorrow morning? I'm gonna [sic] need 16,000 for a very short time with the right kind of terms. I have a very short window to

grab onto something that's of great value to me. And I'm hoping to get a cashier's check ups'd [sic] out tomorrow…

VICTIM 3: Which email address did you send it to?

67. Text message exchange between Duncan and Victim 4 on December 8, 2018:

VICTIM 3: Did you send an addendum for the 2900

DUNCAN: Yes I sent it this morning and just sent it again just now case [sic] you didn't get it. If you still don't have it let me know and I'll stick it in the mail to you.

VICTIM 3: [Auto-Reply] I'm driving right now – I'll get back to you later.

DUNCAN: Ok

VICTIM 3: I haven't checked my e-mail today but I will, thanks.

68. Text message exchange between Duncan and Victim 4 on December 20, 2018:

DUNCAN: Check your email from me

69. Text message exchange between DUNCAN and VICTIM 4 on January 18, 2019:

DUNCAN: Read your email this morning.. --- [sic] copy of My [sic] email from the chairman that I received earlier this morning outlining the nature of the agreement with the Costa Rican cargo company we've just formed a relationship with. I want to get this wrapped up today and money in the Fedex to our person in Maryland … so let me know if your [sic] satisfied with this as soon as you can .. Will need 15000$ cash. And will drive up and pick it up around 230pm if I could. You will still get 125% and an amendment from me even though the risk is -0- because I can do this quickly with you without all the banking formality's – but I will need photo copies of our original agreement and subsequent amendments because I lost a lot of that when my computer

was stolen.

70. Text message exchange between Duncan and Victim 4 on January 11, 2020:

DUNCAN: Saturday – read new Email, all information about the recipient for the Janet wire transfer to Henry Franssen on Monday.

DUNCAN: Please confirm.

71. Text message exchange between Duncan and Victim 4 on January 13, 2020:

DUNCAN: Just wanted to wake you up and remind you that we need to make that transfer at 9:30 this morning and I need you to email me the receipt…

After several other texts, Duncan followed up with Victim 4 on January 13, 2020:

DUNCAN: Please send me an email attachment of the transfer slip. Thank you -/ [sic] Rd01106@Gmail.com

VICTIM 3: It's done

72. According to text messages, wiring instructions or receipts for wire transfers were exchanged between Victim 4 by Duncan on multiple other occasions including February 18, 2020; February 25, 2020; February 29, 2020.

73. Text messages also indicate that email was used by Duncan to communicate with coconspirators not yet known or as a medium to exchange information between coconspirators and victims. Selected examples read as follows:

74. Text message exchange between Duncan and Victim 4 on November 16, 2019:

DUNCAN: ... check your email as I have mailed you a copy of the performance guarantee reconfirmation letter over the signature of the Turkish Kargo [sic] chairman

but we've been working with and also the secretary of the Turkish Kargo [sic]company laying out terms and conditions.

The text message that followed the statement above included a screenshot of a MAC computer screen displaying a letter from Turkish Cargo.

75. Text message exchange between Duncan and Victim 4 on November 16, 2019:

DUNCAN: … the chairman is writing a letter to us now and when he's done it will be mailed to Janet me you and Bob [sic] and will contain language that says we will owe no further money After [sic] our dockage and visa bill is paid… I'll get back to you as soon as I know that this email from the chairman has been sent and is in your email account.

76. According to text messages additional documents were sent to Victim 4 from Duncan via email on February 12, 2020. Text messages also indicate that emails from coconspirators were also forwarded to victims by Duncan on April 8, 2020.

77. In a text message exchange from March 24, 2019 Duncan explains to Victim 4 that he is being audited and requests that they transfer responsibility of tracing the transactions for the investment to Victim 4. In the text exchange Duncan also references his desire to keep his personal email account hidden from investigators, saying "…I'm being audited right now and if they want to check my personal email I wouldn't be too crazy about having that happen…"

TECHNICAL BACKGROUND

78. Based on my Training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name **gmail.com),** like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information.

Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail subscribers) and information concerning subscribers and their use of Gmail services, such as account access information, email transaction information, and account application information. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

79. Additionally, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

80. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email

communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. Also, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

81. Lastly, based on my training and experience, I know that electronic communication sent via email by major service providers often contain header information that include the email address of the sender, the address of the user, internet protocol (IP) addresses of the sender, and the IP address of the recipient or recipients. When combined with other investigative techniques this information can be used to identify the location and identity of the original sender. This information can be used to identify coconspirators or victims as yet unknown to investigators.

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

82. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Yahoo

or Google, as with a conventional warrant, but rather by serving copies of the warrant on the companies and awaiting their production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices. 63. Based on my training and experience and that of other law enforcement officers, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created or received after this 14-day deadline ("latecreated data"). 64. The United States does not ask for this extra data or participate in its production. 23 65. Should Yahoo or Google produce late-created data in response to this warrant, I request permission to view all late-created data that was created by Yahoo or Google, including subscriber, IP address, logging, and other transactional data, without further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the accountholder(s), such as e-mail, absent a follow-up warrant. 66. For these reasons, I request that the Court approve the limitations outlined in the procedures described in Attachment B.

CONCLUSION

83. Based on the forgoing facts and information, I have probable cause to believe that evidence of a violation of 18 U.S.C § 1343, identities of victims, and or information related to identities of conspirators not yet identified will be obtained through the collection of the content of electronic communication for the Gmail account RD01106@gmail.com. I request that the

Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Casey Anderson / KAR

Casey Anderson, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on 08/2/2021

Katherine Robertson

Hon. Katherine A. Robertson
United States Magistrate Judge